IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number	: 09/883,300	Confirmation No.:	9721
Appellant	: Glen Boysko *et al.*		
Filed	: June 19, 2001		
Title	: METHOD AND SYSTEM FOR SECURITY AND USER ACCOUNT INTEGRATION BY REPORTING SYSTEMS WITH REMOTE REPOSITORIE		
TC/Art Unit	: 2155		
Examiner:	: Thu Ha Nguyen		
Docket No.	: 53470.003028		
Customer No.	: **21967**		

APPEAL BRIEF

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number	: 09/883,300	Confirmation No.:	9721
Appellant	: Glen Boysko *et al.*		
Filed	: June 19, 2001		
Title	: METHOD AND SYSTEM FOR SECURITY AND USER ACCOUNT INTEGRATION BY REPORTING SYSTEMS WITH REMOTE REPOSITORIE		
TC/Art Unit	: 2155		
Examiner:	: Thu Ha Nguyen		
Docket No.	: 53470.003028		
Customer No.	: **21967**		

APPEAL BRIEF

In response to the Notice of Panel Decision from Pre-Appeal Brief Review dated June 13, 2008 and the Final Office Action dated January 22, 2008, rejecting claims 1-20, Appellants respectfully request that the Board of Patent Appeals and Interferences reconsider and withdraw the rejections of record, and allow the pending claims, which are attached hereto as an Appendix.

I. REAL PARTY IN INTEREST

The real party in interest is Microstrategy, Inc., the assignee of the above-referenced application.

II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-20 are pending in this application. The rejection of claims 1-20 under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Patent No. 6,453,353 to Win *et al* ("Win") is appealed.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been filed subsequent to the Office Action dated January 22, 2008.

V. SUMMARY OF INVENTION

Appellants believe that a brief discussion of the background technology, followed by a brief summary of the embodiments of the invention and the problems solved by the embodiments of the present invention, will assist the Board of Patent Appeals and Interferences (hereinafter referred to as "the Board") in appreciating the significant advances made by the embodiments of the present invention. Finally, concise explanations of each of the independent claims are provided, including reference to exemplary portions of the specification and figures.

A. The Background

Decision support systems have been developed to efficiently retrieve selected information from data warehouses. One type of decision support system is known as an on-line analytical processing system (OLAP). Other systems may include Business Intelligence and reporting systems. In general, OLAP systems analyze the data from a number of different perspectives and support complex analyses against large input data sets. OLAP systems generally output upon execution of a report that inputs a template to indicate the way to present the output and a filter to specify the conditions of data on which the report is to be presented.

Security is a major concern in any system. Large systems typically provide users with access to a wealth of information, not all of which is meant to be seen by everyone. In general, security systems may have the components related to authentication, access control and auditing. Authentication may include a method for identifying a user to the system. Access control may involve what the user is allowed to see and do once the user has been identified. Auditing may

include a record of the data the user viewed and actions the user performed. Security may be generally implemented in various areas of a system, which may include databases, network/operating systems, and various applications.

Security at the database level is extremely important because anyone can bypass traditional security measures by using a simple, non-secure query tool to access the database or databases. Network controls access to computer while the operating system controls access to the files and applications that are stored in a particular computer. It is important to protect computers, sensitive files and other information from inadvertent or malicious tampering.

B. The Embodiments of The Present Invention

Integration with remote authentication servers may enable a user to access a reporting system wherein the user's account may be integrated with one or more authentication servers of remote systems. The present invention provides security and user account integration with remote authentication servers, (e.g., repositories not owned by the server). Integration may occur with Lightweight Directory Access Protocol (LDAP), an operating system (e.g., Microsoft Windows™ NT™) authentication, custom account repositories and others. For example, the server may synchronize associated user lists with a remote repository. In another example, the server may also make external calls to remote authentication servers to validate a user's username and password. Other information may be validated.

LDAP may relate to a directory-structured way to store data. In particular, many customers may use LDAP to store user information across an organization or customer-base. Rather than creating a new set of users within an entity and/or system, customers may use existing user information stored in LDAP to perform authentication, access checks and other functions.

Customers may use LDAP to authenticate users so that the users may use a single user ID and password. In addition, certificates may be used instead of user ID and password where appropriate. LDAP repositories may store information that describes properties, roles and rights of a user for authorization and other purposes. It may be possible to store vendor-specific information in a LDAP repository and enable applications to read from the LDAP repository rather than from a proprietary data store.

In addition, LDAP may support the concept of groups. For example, during authorization, LDAP groups may be associated with other groups at login. This may remove the need to administer user assignment to groups at both the LDAP and other level. For example, authentication may occur through a web site or other Internet user interface. As a result, the present invention may provide a way to achieve single-sign-on for web and other users.

The present invention provides a method and system for integrating security and user account data in a reporting system with at least one remote repository. A user may submit user credential input to a reporting system. The system may then identify an authentication process. User credential input may be forwarded to a server where the server may apply the authentication process to authenticate the user against a remote repository for verifying the user credential input. User information from the remote repository may be imported. The authentication process may include Lightweight Directory Access Protocol, operating system (e.g., Microsoft Windows™ NT™) authentication and other processes. The server may also synchronize user account data with the user information from the remote repository. In addition, the user may be associated with a group of users wherein group information from the remote repository may be imported. User information may include at least one or user permissions, privileges and access rights associated with the user.

C. Explanation of Independent Claim 1

A method for integrating security and user account data in a reporting system with at least one remote repository (page 2, line 9-17), comprising the steps of:

enabling a user to submit user credential input to a reporting system (page 12, lines 6-9; page 25, lines 1-2);

identifying an authentication process (page 12, line 9 - page 15, line 3; page 25, lines 2-4);

forwarding the user credential input to a first server (page 20, line 17 - page 21, line 2); and

enabling the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying a least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server (page 21, line 11 - page 26, line 17).

D. Explanation of Independent Claim 8

A system for integrating security and user account data in a reporting system with at least one remote repository (page 2, line 9-17), comprising:

an input for enabling a user to submit user credential input to a reporting system (page 12, lines 6-9; page 25, lines 1-2);

an identification module for identifying an authentication process (page 12, line 9 - page 15, line 3; page 25, lines 2-4);

a forwarding module for forwarding the user credential input to a first server (page 20,

line 17 - page 21, line 2); and

a first server for applying the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying a least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server (page 21, line 11 - page 26, line 17).

E. Explanation of Independent Claim 15

A processor-readable medium comprising code for execution by a processor to integrate security and user account data in a reporting system with at least one remote repository (page 2, line 9-17), the medium comprising:

code for causing a processor to enable a user to submit user credential input to a reporting system (page 12, lines 6-9; page 25, lines 1-2);;

code for causing a processor to identify an authentication process (page 12, line 9 - page 15, line 3; page 25, lines 2-4);

code for causing a processor to forward the user credential input to a first server (page 20, line 17 - page 21, line 2); and

code for causing a processor to enable the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying a least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server (page 21, line 11 - page 26, line 17).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues on appeal are whether the following rejection is proper:

The rejection of claims 1-20 under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Patent No. 6,453,353 to Win *et al* ("Win").

VII. ARGUMENT

The rejections against the pending claims under consideration in the above-identified patent application should be reversed for at least the reasons set forth below.

A. Brief Description of the Art Applied to the Claims

U.S. Patent No. 6,453,353 to Win *et al* ("Win").

Win purports to disclose a network using role-based navigation among protected information resources (col. 1, lines 11-15). More specifically, Win appears to discuss a method and apparatus for controlling access to protected information resources by enabling organizations to register information sources and user information in a central repository (col. 5, lines 12-14). Win purports to allow administrators to implement access rules by defining roles that users play when working for an organization or doing business with an enterprise, thus forming an additive data model (col. 5, lines 21-23, 57-58).

B. The Rejection of Claims 1-20 Under 35 U.S.C. § 102(e) is Improper

Claims 1-20 stand rejected under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Patent No. 6,453,353 to Win *et al* ("Win"). Appellants respectfully traverse this rejection.

1. Claim 1 is Separately Patentable

The rejection is improper because **Win fails to teach each and every claim limitation** for claim 1 rejected under 102(e).

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id.. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). Such possession is effected only if one of ordinary skill in the art could have combined the disclosure in the prior art reference with his/her own knowledge to make the claimed invention. Id.. As stated in MPEP § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Referring to claim 1, the disclosure of Win fails to show at least the limitation directed to "enabling the first server...*to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects*, wherein the remote repository is located ***within*** a second server, the second server being different from the first server"(emphasis added).

Specifically, Win makes no mention of a applying the authentication process to against "a ***remote*** repository" and "wherein the remote repository is located ***within*** a second server, the second server being different from the first server" (emphasis added). In fact, Win appears to merely teach that resource and user information are organized in a "central repository." *See* Win

at col. 5, lines 12-20. This is clearly distinguishable from a remote repository that is not owned by the server.

Furthermore, even assuming that Win teaches a remote repository, Win clearly teaches that the repository is not "located within" the second server, as expressly recited in claim 1. Rather, the "Registry Server 108 is **coupled to** a Registry Repository 110" (emphasis added). *See* Win at col. 6, lines 20-26. Although this argument has been previously presented to the Office, the Office has continued to deliberately misconstrue the Win reference without any explanation. For instance, Win expressly recites that its "Registry Server 108 is **coupled to** a Registry Repository 110" (emphasis added); however, the Office conveniently refers Win as teaching a "registry repository 110 **at the** registry server 108" (emphasis added). *Office Action* at p. 2 and 4. This is clearly not what is shown in Win and therefore an improper application of the reference under section 102.

In addition, not only does Win fail to teach a remote repository that is located within a second server, Win also fails to teach the step of determining user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects. In fact, Win appears to merely teach a role-specific access ***menu*** to a network user that is ***available to show only*** those resources that the user is authorized to access according to the user's profile information, including roles and privileges. *Office Action* at p. 4 (citing Win, col. 5, line 66 - col. 6, line 17, "providing user a personalized menu that displays only resources that user has a right to access"). This is clearly distinguishable from access control data for identifying at least one user privilege for ***performing one or more actions*** and at least one user permission associated with one or more objects.

As a result, the disclosure of Win fails to teach or show at least the limitation directed to

"enabling the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and ***to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server***," as expressly recited in claim 1.

Accordingly, for at least this reason, Win does not teach **each and every limitation** of claim 1 and the rejection of claim under 35 U.S.C. § 102(e) should be withdrawn.

Therefore, independent claim 1 is allowable over Win and allowance thereof is respectfully requested.

2. Claim 2 is Separately Patentable

Claim 2 is separately patentable because Win is not prior art and fails to disclose importing user information from the remote repository. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 1. Win fails to show each and every limitation of claim 2. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 2 be withdrawn.

3. Claim 3 is Separately Patentable

Claim 3 is separately patentable because Win is not prior art and fails to disclose the authentication process comprises Lightweight Directory Access Protocol. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 1. Win fails to show each and every limitation of claim 3. In addition, there is no teaching, motivation,

or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 3 be withdrawn.

4. Claim 4 is Separately Patentable

Claim 4 is separately patentable because Win is not prior art and fails to disclose the authentication process comprises an operating system authentication. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 1. Win fails to show each and every limitation of claim 4. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 4 be withdrawn.

5. Claim 5 is Separately Patentable

Claim 5 is separately patentable because Win is not prior art and fails to disclose enabling the server to synchronize user account data with the user information from the remote repository. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 1. Win fails to show each and every limitation of claim 5. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 5 be withdrawn.

6. Claim 6 is Separately Patentable

Claim 6 is separately patentable because Win is not prior art and fails to disclose the user is associated with a group of users wherein group information from the remote repository is

imported. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 1. Win fails to show each and every limitation of claim 6. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 6 be withdrawn.

7. Claim 7 is Separately Patentable

Claim 7 is separately patentable because Win is not prior art and fails to disclose the user information comprises at least one or user permissions, privileges and access rights associated with the user. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 1. Win fails to show each and every limitation of claim 7. In addition, there is no teaching or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellant respectfully requests that the rejection of claim 7 be withdrawn.

8. Claim 8 is Separately Patentable

The rejection is improper because **Win fails to teach each and every claim limitation** for claim 8 rejected under 102(e).

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id.. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471,

1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). Such possession is effected only if one of ordinary skill in the art could have combined the disclosure in the prior art reference with his/her own knowledge to make the claimed invention. Id.. As stated in MPEP § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Referring to claim 8, the disclosure of Win fails to show at least the limitation directed to "a first server...*to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects*, wherein the remote repository is located ***within*** a second server, the second server being different from the first server"(emphasis added).

Specifically, Win makes no mention of a applying the authentication process to against "a ***remote*** repository" and "wherein the remote repository is located ***within*** a second server, the second server being different from the first server" (emphasis added). In fact, Win appears to merely teach that resource and user information are organized in a "central repository." *See* Win at col. 5, lines 12-20. This is clearly distinguishable from a remote repository that is not owned by the server.

Furthermore, even assuming that Win teaches a remote repository, Win clearly teaches that the repository is not "located within" the second server, as expressly recited in claim 1. Rather, the "Registry Server 108 is **coupled to** a Registry Repository 110" (emphasis added).

See Win at col. 6, lines 20-26. Although this argument has been previously presented to the Office, the Office has continued to deliberately misconstrue the Win reference without any explanation. For instance, Win expressly recites that its "Registry Server 108 is **coupled to** a Registry Repository 110" (emphasis added); however, the Office conveniently refers Win as teaching a "registry repository 110 **at the** registry server 108" (emphasis added). *Office Action* at p. 2 and 4. This is clearly not what is shown in Win and therefore an improper application of the reference under section 102.

In addition, not only does Win fail to teach a remote repository that is located within a second server, Win also fails to teach the step of determining user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects. In fact, Win appears to merely teach a role-specific access ***menu*** to a network user that is ***available to show only*** those resources that the user is authorized to access according to the user's profile information, including roles and privileges. *Office Action* at p. 4 (citing Win, col. 5, line 66 - col. 6, line 17, "providing user a personalized menu that displays only resources that user has a right to access"). This is clearly distinguishable from access control data for identifying at least one user privilege for ***performing one or more actions*** and at least one user permission associated with one or more objects.

As a result, the disclosure of Win fails to teach or show at least the limitation directed to "a first server for applying the authentication process to authenticate the user against a remote repository for verifying the user credential input and ***to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server***," as expressly

recited in claim 8.

Accordingly, for at least this reason, Win does not teach **each and every limitation** of claim 8 and the rejection of claim under 35 U.S.C. § 102(e) should be withdrawn.

Therefore, independent claim 1 is allowable over Win and allowance thereof is respectfully requested.

9. Claim 9 is Separately Patentable

Claim 9 is separately patentable because Win is not prior art and fails to disclose an import module for importing user information from the remote repository. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 8. Win fails to show each and every limitation of claim 9. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 9 be withdrawn.

10. Claim 10 is Separately Patentable

Claim 10 is separately patentable because Win is not prior art and fails to disclose the authentication process comprises Lightweight Directory Access Protocol. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 8. Win fails to show each and every limitation of claim 10. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 10 be withdrawn.

11. Claim 11 is Separately Patentable

Claim 11 is separately patentable because Win is not prior art and fails to disclose the

authentication process comprises an operating system authentication. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 8. Win fails to show each and every limitation of claim 11. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 11 be withdrawn.

12. Claim 12 is Separately Patentable

Claim 12 is separately patentable because Win is not prior art and fails to disclose the server synchronizes user account data with the user information from the remote repository. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 8. Win fails to show each and every limitation of claim 12. In addition, there is no teaching or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellant respectfully requests that the rejection of claim 12 be withdrawn.

13. Claim 13 is Separately Patentable

Claim 13 is separately patentable because Win is not prior art and fails to disclose the user is associated with a group of users wherein group information from the remote repository is imported. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 8. Win fails to show each and every limitation of claim 13. In addition, there is no teaching or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellant respectfully requests that the rejection of claim

13 be withdrawn.

14. Claim 14 is Separately Patentable

Claim 14 is separately patentable because Win is not prior art and fails to disclose the user information comprises at least one or user permissions, privileges and access rights associated with the user. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 8. Win fails to show each and every limitation of claim 14. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 14 be withdrawn.

15. Claim 15 is Separately Patentable

The rejection is improper because **Win fails to teach each and every claim limitation** for claim 15 rejected under 102(e).

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id.. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). Such possession is effected only if one of ordinary skill in the art could have combined the disclosure in the prior art reference with his/her own knowledge to make the claimed

invention. Id.. As stated in MPEP § 2131, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Referring to claim 15, the disclosure of Win fails to show at least the limitation directed to "code for causing a processor to enable the first server...*to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects*, wherein the remote repository is located ***within*** a second server, the second server being different from the first server"(emphasis added).

Specifically, Win makes no mention of a applying the authentication process to against "a ***remote*** repository" and "wherein the remote repository is located ***within*** a second server, the second server being different from the first server" (emphasis added). In fact, Win appears to merely teach that resource and user information are organized in a "central repository." *See* Win at col. 5, lines 12-20. This is clearly distinguishable from a remote repository that is not owned by the server.

Furthermore, even assuming that Win teaches a remote repository, Win clearly teaches that the repository is not "located within" the second server, as expressly recited in claim 1. Rather, the "Registry Server 108 is **coupled to** a Registry Repository 110" (emphasis added). *See* Win at col. 6, lines 20-26. Although this argument has been previously presented to the Office, the Office has continued to deliberately misconstrue the Win reference without any explanation. For instance, Win expressly recites that its "Registry Server 108 is **coupled to** a Registry Repository 110" (emphasis added); however, the Office conveniently refers Win as teaching a "registry repository 110 **at the** registry server 108" (emphasis added). *Office Action*

at p. 2 and 4. This is clearly not what is shown in Win and therefore an improper application of the reference under section 102.

In addition, not only does Win fail to teach a remote repository that is located within a second server, Win also fails to teach the step of determining user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects. In fact, Win appears to merely teach a role-specific access ***menu*** to a network user that is ***available to show only*** those resources that the user is authorized to access according to the user's profile information, including roles and privileges. *Office Action* at p. 4 (citing Win, col. 5, line 66 - col. 6, line 17, "providing user a personalized menu that displays only resources that user has a right to access"). This is clearly distinguishable from access control data for identifying at least one user privilege for ***performing one or more actions*** and at least one user permission associated with one or more objects.

As a result, the disclosure of Win fails to teach or show at least the limitation directed to "code for causing a processor to enable the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and ***to determine user access control data for identifying at least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server***," as expressly recited in claim 15.

Accordingly, for at least this reason, Win does not teach **each and every limitation** of claim 1 and the rejection of claim under 35 U.S.C. § 102(e) should be withdrawn.

Therefore, independent claim 15 is allowable over Win and allowance thereof is respectfully requested.

16. Claim 16 is Separately Patentable

Claim 16 is separately patentable because Win is not prior art and fails to disclose code for causing a processor to import user information from the remote repository. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 15. Win fails to show each and every limitation of claim 16. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 16 be withdrawn.

17. Claim 17 is Separately Patentable

Claim 17 is separately patentable because Win is not prior art and fails to disclose the authentication process comprises at least one of Lightweight Directory Access Protocol and operating system authentication. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 15. Win fails to show each and every limitation of claim 17. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 17 be withdrawn.

18. Claim 18 is Separately Patentable

Claim 18 is separately patentable because Win is not prior art and fails to disclose code for causing a processor to enable the server to synchronize user account data with the user information from the remote repository. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 15. Win fails to show each and every

limitation of claim 18. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 18 be withdrawn.

19. Claim 19 is Separately Patentable

Claim 19 is separately patentable because Win is not prior art and fails to disclose the user is associated with a group of users wherein group information from the remote repository is imported. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 15. Win fails to show each and every limitation of claim 19. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 19 be withdrawn.

20. Claim 20 is Separately Patentable

Claim 20 is separately patentable because Win is not prior art and fails to disclose the user information comprises at least one or user permissions, privileges and access rights associated with the user. The Office Action's rejection of this claim is improper for the reasons set forth above with respect to claim 15. Win fails to show each and every limitation of claim 20. In addition, there is no teaching, motivation, or rationale of obviousness to modify any of the applied references to include this feature.

For at least the above reasons Appellants respectfully request that the rejection of claim 20 be withdrawn.

VIII. CONCLUSION

Accordingly, Appellants respectfully requests that the Board reverse the prior art rejections set forth in the Final Office Action. The Director is hereby authorized to treat any current or future reply, requiring a petition for an extension of time for its timely submission as incorporating a petition for extension of time for the appropriate length of time. Appellants also authorize the Director to credit and differences or overpayment of fees to the undersigned's Deposit Account No. 50-0206.

Respectfully submitted,

Date: July 9, 2008

Brian M. Buroker
Registration No. 39,125

Hunton & Williams, LLP
1900 K. St., NW, Suite 1200
Washington, D.C. 20006-1109
Tel. (202) 955-1894
Fax (202) 778-2201

IX. CLAIMS APPENDIX

1. (Previously presented) A method for integrating security and user account data in a reporting system with at least one remote repository, comprising the steps of:

enabling a user to submit user credential input to a reporting system;

identifying an authentication process;

forwarding the user credential input to a first server; and

enabling the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying a least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server.

2. (Original) The method of claim 1 further comprising a step of importing user information from the remote repository.

3. (Original) The method of claim 1 wherein the authentication process comprises Lightweight Directory Access Protocol.

4. (Original) The method of claim 1 wherein the authentication process comprises an operating system authentication.

5. (Original) The method of claim 2 further comprising a step of enabling the server to synchronize user account data with the user information from the remote repository.

6. (Original) The method of claim 1 wherein the user is associated with a group of users wherein group information from the remote repository is imported.

7. (Original) The method of claim 2 wherein the user information comprises at least one

or user permissions, privileges and access rights associated with the user.

8. (Previously presented) A system for integrating security and user account data in a reporting system with at least one remote repository, comprising:

an input for enabling a user to submit user credential input to a reporting system;

an identification module for identifying an authentication process;

a forwarding module for forwarding the user credential input to a first server; and

a first server for applying the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying a least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server.

9. (Original) The system of claim 8 further comprising an import module for importing user information from the remote repository.

10. (Original) The system of claim 8 wherein the authentication process comprises Lightweight Directory Access Protocol.

11. (Original) The system of claim 8 wherein the authentication process comprises an operating system authentication.

12. (Original) The system of claim 9 wherein the server synchronizes user account data with the user information from the remote repository.

13. (Original) The system of claim 8 wherein the user is associated with a group of users wherein group information from the remote repository is imported.

14. (Original) The system of claim 9 wherein the user information comprises at least one or user permissions, privileges and access rights associated with the user.

15. (Previously presented) A processor-readable medium comprising code for execution by a processor to integrate security and user account data in a reporting system with at least one remote repository, the medium comprising:

code for causing a processor to enable a user to submit user credential input to a reporting system;

code for causing a processor to identify an authentication process;

code for causing a processor to forward the user credential input to a first server; and

code for causing a processor to enable the first server to apply the authentication process to authenticate the user against a remote repository for verifying the user credential input and to determine user access control data for identifying a least one user privilege for performing one or more actions and at least one user permission associated with one or more objects, wherein the remote repository is located within a second server, the second server being different from the first server.

16. (Original) The medium of claim 15 further comprising code for causing a processor to import user information from the remote repository.

17. (Original) The medium of claim 15 wherein the authentication process comprises at least one of Lightweight Directory Access Protocol and operating system authentication.

18. (Original) The medium of claim 16 further comprising code for causing a processor to enable the server to synchronize user account data with the user information from the remote repository.

19. (Original) The medium of claim 15 wherein the user is associated with a group of users wherein group information from the remote repository is imported.

20. (Original) The medium of claim 16 wherein the user information comprises at least

one or user permissions, privileges and access rights associated with the user.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.